Escalation to Client or Customer

Any employee or contractor who discovers any event of a questionable, fraudulent, or illegal nature should:

1. Report the situation via Slack or email to our Incident Response Team, which is defined in the Incident Response Policy.
2. Fill out the incident report form.

These reports should be made without fear of retaliation.

The incident response team will evaluate the incident and determine whether to notify the client. Situations that require escalation to the client include:

- System intrusion - software exploit, SQL injection, XSS, use of stolen credentials.
- Malware - ransomware, worm, spyware, rootkits, etc.
- Information gathering - reconnaissance activities, network scanning or sniffing.
- Social engineering - phishing, bribes and other (physical) threats
- Fraud or theft
- Unauthorized use of system privileges
- Information breach
- Other incidents categorized as high or critical in severity

Timeline

When an incident has occurred, Nested Knowledge will notify the client or customer within 2 hours for High-Severity incidents and within 40 minutes for Critical incidents.

Incident categorization is described in our Incident Response Policy.

Roles

Our Incident Response Team, consisting of the CEO, CTO, and COO, will notify the appropriate client or customer agency via email.

Communication and Compliance

All investigators and leads on the Incident Response Team will be required to review this policy. This policy will be updated on an annual basis. Employees who deliberately violate this policy will be subject to disciplinary action up to and including termination.

Revision History

Author	Date of Revision/Review	Comments/Description
K. Cowie	01/24/2023	Reviewed
K. Kallmes	11/19/2021	Draft approved

Return to Policies